13th ICCRTS
"C2 for Complex Endeavors"

Network Science: Observations from the Omni Fusion 2007 Digital Warfighter Exercise Simulation Experiment

Jeffrey A. Thomas
U.S. Army Research Laboratory
Human Research and Engineering Directorate
Aberdeen Proving Ground
Jeffrey.alexander.thomas@us.army.mil

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE **JUN 2008**	2. REPORT TYPE	3. DATES COVERED **00-00-2008 to 00-00-2008**

4. TITLE AND SUBTITLE **Network Science: Observations from the Omni Fusion 2007 Digital Warfighter Exercise Simulation Experiment**	5a. CONTRACT NUMBER 5b. GRANT NUMBER 5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER 5e. TASK NUMBER 5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U.S. Army Research Laboratory,Human Research and Engineering Directorate,Aberdeen Proving Ground,MD,21005**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR’S ACRONYM(S) 11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

13th International Command and Control Research and Technology Symposia (ICCRTS 2008), 17-19 Jun 2008, Seattle, WA

14. ABSTRACT

Net-centric operations depend on the development of coherent systems of interacting networks using rapidly evolving information technologies, doctrine, and training paradigms (National Research Council, 2005). To this end, research and experimentation are required to understand the organizational processes and procedures required to enable network command and control (C2). This paper details the application of network science to understand human network interactions in a recent command and control simulation experiment, the Omni Fusion 2007 Experiment/Digital Warfighting Exercise Block III (OF07/DWE III) simulation exercise (SIMEX). This paper describes research and analyses about the promulgation of situation awareness (SA) and understanding throughout a Division and subordinate Brigade organizations. Social network analysis (SNA) was used to help determine the structure of human relations and to express that structure in network form. The SA data collected and the results from the SNA, taken together, assisted in understanding organizational networks, networking technology capabilities, and intra-and inter-team processes facilitating the development of SA among distributed and collocated commanders and staff within the refined modular division.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**14**	

Network Science: Observations from the Omni Fusion 2007 Digital Warfighter Exercise Simulation Experiment

Jeffrey A. Thomas
U.S. Army Research Laboratory
Human Research and Engineering Directorate
Aberdeen Proving Ground, MD 21005
Jeffrey.alexander.thomas@arl.army.mil

Abstract

Net-centric operations depend on the development of coherent systems of interacting networks using rapidly evolving information technologies, doctrine, and training paradigms (National Research Council, 2005). To this end, research and experimentation are required to understand the organizational processes and procedures required to enable network command and control (C2). This paper details the application of network science to understand human network interactions in a recent command and control simulation experiment, the Omni Fusion 2007 Experiment/Digital Warfighting Exercise Block III (OF07/DWE III) simulation exercise (SIMEX). This paper describes research and analyses about the promulgation of situation awareness (SA) and understanding throughout a Division and subordinate Brigade organizations. Social network analysis (SNA) was used to help determine the structure of human relations and to express that structure in network form. The SA data collected and the results from the SNA, taken together, assisted in understanding organizational networks, networking technology capabilities, and intra-and inter-team processes facilitating the development of SA among distributed and collocated commanders and staff within the refined modular division.

Keywords: Network Science, Situation Awareness, Social Network Science

I. Introduction

Generally speaking, battles of every kind are won primarily on two principles: the quality of information and whether or not this information is properly used. For example, inaccurate, incomplete, or untimely information has caused many people to loose their battle to cancer (i.e. inaccurate or late diagnosis of cancer); led to catastrophic accidents (i.e. U.S. Vincennes and Stark); and have brought nations extremely close to war (i.e. The Bay of Pigs).

Information quality and its proper use have also become integral in the evolution of military doctrine. For more than a decade the U.S. Department of Defense (DoD) formally recognized that information and the skillful manipulation of information is a strategic asset (DoD Directive 3600.1, 1992, cited in Fredericks, 1997). More recently, the importance of information is evident in current military doctrine across many nations. Alberts, Garstka and Stein (1999) note that Network Centric Warfare (NCW), Network Centric Operations (NCO), or Network Enabled Capability (NEC) recognizes the need to co-evolve an approach to command and control (C2) that takes advantage of the proliferation of information.

One approach the U.S. DoD has taken to capitalize on rapidly changing information is in developing and adapting highly sophisticated information management technologies. Technologies such as the Command Post of the Future (CPOF), Force XXII Battle Command Brigade and Below (FBCB2), and Army Battle Command Systems (ABCS) are being developed and fielded to provide improved information management and information exchange capabilities to Commanders and staff. These technologies are said to provide the Commander and staff greater battlespace awareness to improve their situational awareness (SA) and decision making abilities. These kinds of information systems show promise in today's complex and dynamic information-rich environment. However, information systems in and of themselves do not win wars; people do. Wars are won based in large part with humans using information systems and supporting technologies and developing procedures for managing and fusing information – also referred to as the human dimension of networking. The need to address the human dimension of networking is noted by the National Research Council's Board on Army Science and Technology: "Battlefield reports and analyses show that current information systems used by the Army and other services need to be improved and integrated into a solution encompassing the physical, cognitive, and social domains" (National Research Council, 2005, p. 21).

To better understand the human dimension of networking it is important to visit the concept of NCO. NCO depends on the development of coherent systems of interacting networks using rapidly evolving information technologies (National Research Council, 2005). It is believed that these technologies help produce more accurate, timely and complete information. These technologies also are believed to provide a means to provide the right information to the right person at the right time - a process known as networking. Taken together, networking is the study of people developing and implementing processes and their use of information management technologies to exchange information. As shown in the figure 1, the value of NCO capabilities is fully realized in the cognitive and social domains – the human dimension of networking. The cognitive domain is where participants are processing and interacting with incoming information to make sense of their situation. The social domain is where people, processes, and their use of technologies intersect**.** The relationship between these domains is presented in the Conceptual Framework Version 2.0 where "People perceive information in the cognitive domain and turn it into knowledge in the social domain (Garstka and Alberts, 2004, 19).

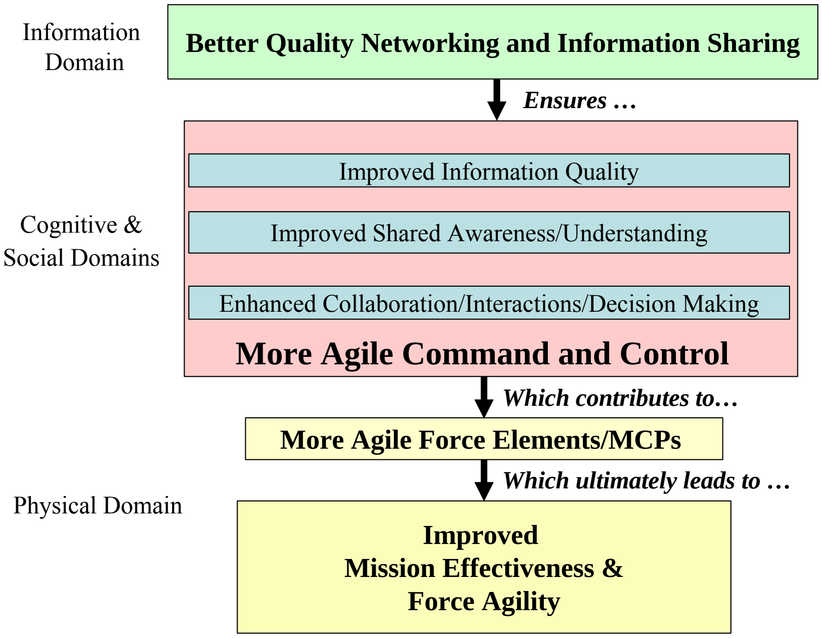
Information Domain
Better Quality Networking and Information Sharing
Ensures …
Cognitive & Social Domains
Improved Information Quality
Improved Shared Awareness/Understanding
Enhanced Collaboration/Interactions/Decision Making
More Agile Command and Control
Which contributes to…
More Agile Force Elements/MCPs
Which ultimately leads to …
Physical Domain
Improved Mission Effectiveness & Force Agility

Figure 1: Value of Network-Centric Capabilities

The quality of information effects SA. Likewise, the overarching network structure impacts information sharing which in-turn affects SA. If either the network structure or the information quality is degraded, one can expect a resulting impact on mission effectiveness. Additional research is needed to help determine the degree of the cause-and-effect relationship. To this end, research and experimentation are required to understand the organizational processes and procedures required to enable network C2. This paper details the application of network science to understand human network interactions in a recent command and control simulation experiment, the Omni Fusion 2007 Experiment/Digital Warfighting Exercise Block III (OF07/DWE III) simulation exercise (SIMEX). The author describes research and analyses about the promulgation of situation awareness (SA) throughout a Division and subordinate Brigade organizations. Social network analysis (SNA) was used to help determine the structure of human relations and to express that structure in network form. The SA data collected and the results from the SNA, taken together, assisted in understanding organizational networks, networking technology capabilities, and intra-and inter-team processes facilitating the development of SA among distributed and collocated Commanders and staff within the refined modular division.

II. The Digital Warfighting Exercise

The Omni Fusion 2007 Experiment/Digital Warfighting Exercise Block III (OF07/DWE III) simulation exercise (SIMEX) provided an opportunity to assess the capability of the refined modular division to command and control full spectrum operations in a human-in-the-loop (HITL) simulation. Although the simulation exercise was organized under three main issues, the first two are directly related to the research discussed in the paper.

The first objective was to identify the implications associated with commanding and controlling the refined modular division as it transitions from major combat operations to stability operations. The second objective was to identify the intelligence, surveillance, and reconnaissance (ISR) implications when a Battlefield Surveillance Brigade (BFSB) cannot collect data in the division's unassigned areas (areas not assigned to subordinate brigade) and the ability of the BFSB to command and control (C2) augmented maneuver and support forces. Finally, the third objective identified the interoperability requirements for the refined modular division (version 8.0) when conducting coalition operations.

The Georgia, Armenia, Azerbaijan, Turkey (GAAT, unclassified) scenario was used in this exercise. The GAAT scenario is set in a historically unstable region of factionalism, ethnic animosity, religious unrest, and hostility to U.S.-led military forces. At the start of the exercise, the 4th Infantry Division (4ID) had completed major combat operations and had defeated the major combat forces within the area of operation and, simultaneously, a diplomatic agreement created a zone of separation (ZOS) between friendly and defeated enemy forces.

One-hundred and twenty-five (125) role-players performed C2 functions in response to scripted events developed in a master scenario event list (MSEL). As the exercise began, MSELs were electronically sent to higher and subordinate units (response cells). Each MSEL contained information about battlefield events. Each role-player was expected to integrate this information into their existing understanding about the enemy situation while performing a variety of tasks. These tasks included:

1. Conduct physical security operations in the Division AO to reestablish and sustain the rule of law
2. Assess, train, advise and assist Azeri (AZ) forces (military and civil police) to assume the security mission
3. Begin the restoration of essential services - sewage, water, electricity, academics, and trash (SWEAT) - to the Azeri people, working with Azeri officials for them to assume this role
4. Secure the international border
5. Conduct surveillance of activities in the ZOS and along the international border
6. Conduct an Information Warfare campaign
7. Disarm the enemy

The Command Post of the Future (CPOF) system was the primary battle command interface used for command and control during the exercise. CPOF is a decision support system that provides battlespace data and also a means of collaboration among commanders and their staffs to support decision making. Figure 2 shows a snap-shot of the Division common operating picture (COP) provided by CPOF.

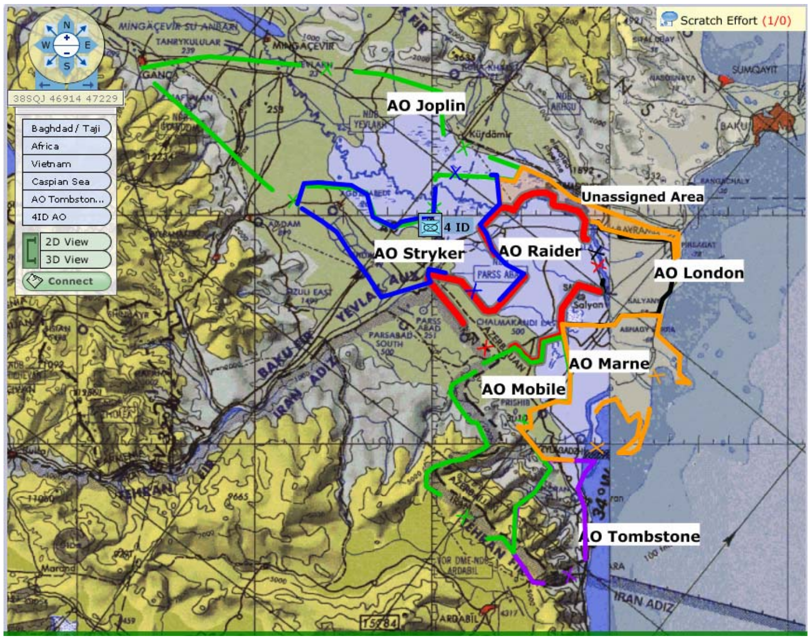

Figure 2: Common Operations Picture from CPOF

III. Method

A. Participants

The OF07/DWE III simulation exercise (SIMEX) involved 125 role-players representing experimental control staff, analysts, Division, and supporting or response brigades (Figure 3). For purposes of this study, data collection and analysis were focused on the activities and interactions of the Division and the BFSB role-players, a total of 58 participants.

Every role-player received a week of on-site classroom training on operating CPOF. During this time, scenario details were briefed. This briefing included details about the current situation, enemy intent, enemy and friendly locations, potential threats to mission success, and the perceived social and political climate of internally displaced persons (IDPs). This detail training helped to ensure everyone had a near equal understanding about the current situation before the start of the simulation exercise. This training period also gave the role-players a chance to become familiar with their assigned roles and to begin developing standard operating procedures for technology use for information management and sharing.

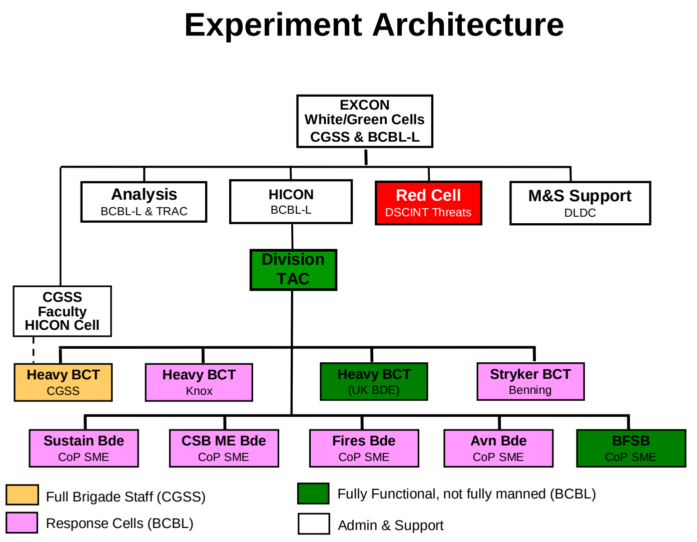

Figure 3, OF07/DWE III SIMEX Experiment Architecture

B. Data Collection

Data were collected using two types of audit trail measures: situation awareness (SA) probes and social \ dynamic network analysis (S\DNA) surveys. Sixteen (16) surveys were administered throughout the four day experiment; eight SA and eight S\DNA. The SA surveys were made-up of six different true - false statements (probes) broken down by three major information categories: 1) knowledge of the commander's intent (CI), 2) awareness of critical scenario events, and 3) knowledge about task specific roles and responsibilities. In total, role players responded to 48 true - false probes using the Information Dissemination Management Tool (IDMT). Each SA probe was carefully written and cross-checked against a set of written expectations provided by the experimental staff and the MSEL team. Knowledge about each MSEL and the key tasks to be performed by the Division and the supporting elements provided a reliable means for capturing ground truth. Furthermore, this additional layer of cooperation between the MSEL writers and the author helped to ensure each SA probe was directly relevant to the three major research issues and relevant to the key tasks of the Division and BFSB.

This approach to measuring SA is a development of the QUASA^{TM} method (QUantitative Analysis of Situation Awareness; Edgar et al., 2000, 2003; McGuiness, 2004 and Leggatt, 2004) and has been used in a previous study by the author (Thomas et al., 2006). The QUASA^{TM} method uses basic probe statements about the situation requiring participants to judge whether each statement is true or false. Participant responses can be interpreted using the Signal Detection Theory (SDT) paradigm which allows the analyst to calculate individual statistics on hits, misses, false alarms, and correct rejections.

After the data are categorized, commonly used SDT statistics can be applied: sensitivity (d') and bias (β). These measures provide a means to assess individual abilities to distinguish between true and false information, represented by the presupposition that battlefield SA involves the combination of both true and false information. Good SA is defined as having the ability to distinguish the two types of information (Edgar et al., 2003). Therefore, the greater someone's sensitivity (d'), the better they are at identifying the signal (true probe) from the noise (false probe).

Social \ Dynamic Network Analysis (S\DNA) is a mathematical, systematic analysis of empirical data to determine the structure of human relations and to express that structure in network form. S\DNA was conducted to determine role player interaction and identify the critical information nodes within the division. Data were collected through a twice daily survey in which all players reported their most frequent communication partners since the previous survey. This analysis identified the key roles that tended to accumulate information, facilitate information flows, and influence organizational outcomes more than the other roles by calculating centrality measures: degree centrality, betweeness centrality, and closeness centrality.

Social network researchers study organizational behavior by examining network activity using the concept of degrees - the number of direct connections a node has. The measure of degree centrality indicates if a node is considered a hub in the network. This node (or role-player in the context of this experiment) is the person with the greatest number of opportunities to exchange information. The betweeness centrality measure measures a role-player's linkages between two larger sub-networks. This person has the greatest influence over what information is exchanged in the network. Closeness centrality is a measure of someone's access to others in the network. Essentially, a greater degree of closeness indicates that they are a key component of the network and is therefore in an excellent position to monitor the information flow in the network.

IV. Results and Discussion

A. Situation Awareness

Due to incomplete survey responses, SA results are only available for 29 participants, 50% of the target audience (N = 58). Results from the sensitivity analysis suggest that the technologies used in this experiment were not statistically different in allowing role players performing separate tasks to gather, fuse, and synthesize information and make inferences about the validity of the information (Figure 4).

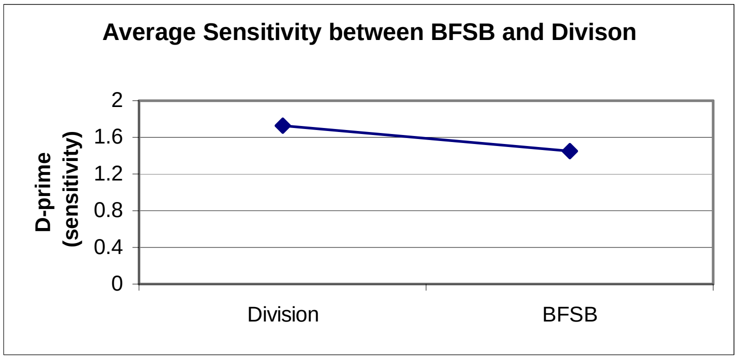

Figure 4: Average Sensitivity (d'prime) between BFSB and Division

A simple scatter plot shows a general decline in the average abilities of participants in the Division and BFSB to distinguish between true and false information (Figure 5).

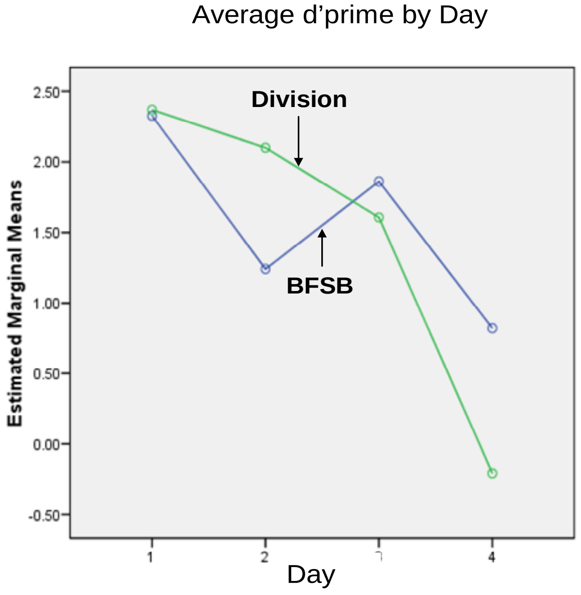

Figure 5: Division and BFSB Average Sensitivity (d') by Day

In the real-world this decline in sensitivity (d') would not be desirable. However, the artificiality of an experiment does explain why individual sensitivities (d') on average would be higher in the beginning of the experiment when there has been very little new information from the simulation to process and integrate into an existing understanding about current battlefield events. Naturally, as the experiment continued and events unfolded, participants were forced to re-focus and respond to new information about the battlefield environment. As more time passes, information most often becomes outdated and participants become overwhelmed as they must process new information and integrate this information into their existing understanding about battlefield events. This makes it much harder to distinguish between true and false information.

The figure above also shows another interesting pattern. Although the average sensitivities (d') within the BFSB dropped on the second day, sensitivity rebounded slightly on the third. This effect may be due to a simulation failure on the second day of experimentation. Many participants reported they were unaware that the simulation stopped running. This simulation failure provided a rich opportunity where current and ongoing decision making could have been based on out dated, inaccurate, or incomplete information. This simulation failure also affected the overall communication network, as results from S\DNA indicate.

Descriptive statistics for each of the three information categories that the true/false (T/F) statements represent are provided below. Division role players (n = 25) achieved a score of 84% for correctly assessing all probe statements about the Division Commander's Intent. The Division staff's performance is largely due to the potential conflicts the BFSB role players (n = 5) encountered as they had competing tasks of meeting the division commander's critical information requirements/priority information requirements, and responding to events in their separate area of operations (AO).

When asked about scenario events, role-players in both the Division and BFSB were correct 64% of the time. This suggests that that both the BFSB and Division staffs were equally "aware" of the unfolding events within their AOs.

BFSB role-players were better aware of their assigned roles and responsibilities and how they related to the overall mission as compared to the Division. When asked about roles and responsibilities, the BFSB accurately judged statements about their roles and responsibilities 67% of the time during the exercise. The Division responses were correct 56% of the time. These results also suggest that the BFSB staff understood their roles and responsibilities slightly better than the division staff. This could be expected as the BFSB was more specialized and given a much narrow focus as compared to the Division staff who performed a wider variety of tasks in support of the mission objectives.

B. Social \ Dynamic Network Analysis

The lack of differences in the sensitivity scores previously reported in Figure 4 may be explained using social \ dynamic network analysis (S\DNA). For example, results in Figure 6 show that the Division G7, Information Operations Officer, was critical to information flow. The G7 was a special staff role in that this role player's primary function was to facilitate information flow throughout the division staff and push information down to supporting elements, such as the BFSB. The G7 was observed coordinating actions and responding to requests for information. This explains why the G7 is among the highest in betweenness centrality (0.103).

Role	Betweenness Centrality
Division Assistant Chief of Staff for Logistics (G4)	**0.107**
Division informations Officer (G7)*	**0.103***
Division Chief of Plans	**0.098**
Division Fires Support Coordinator	**0.092**
Division Intelligences Officer (G2)	**0.083**
Division Commander	**0.061**
Division Air Missile	**0.057**
Division Operations Officer (G3)	**0.041**

Figure 6: Betweenness Centrality – Top 8 Rankings of the Division Roles Performing Most Important Communications across All Days

Additional S\DNA results also show that the overall command organization communications structure was both highly connected and central in the first day of experimentation (Figures 7 and 8). In other words, Figure 7 shows the effect of a physical network failure on a formal communication structure. When the physical network was intact and the simulation was running, the degree of communications between distributed and collocated members remained high. During the second day of simulation, the physical communications network failure negatively impacted the overall communications structure. Distributed participants within the Division and the BFSBs were unable to receive and exchange vital information about the battlespace environment with other members in their staffs.

However, Figure 8 shows that when the simulation failed, the overall command organization including the BFSB and subordinate Brigades flattened. By flattening the communication structure, the overall organization lessened its reliance upon central nodes for maintaining information exchange and SA. It was observed that most role players were not aware that the simulation outage had occurred. Nonetheless, flattening the communication structure is a demonstration of adaptability and resiliency of the overall command organization during a network failure.

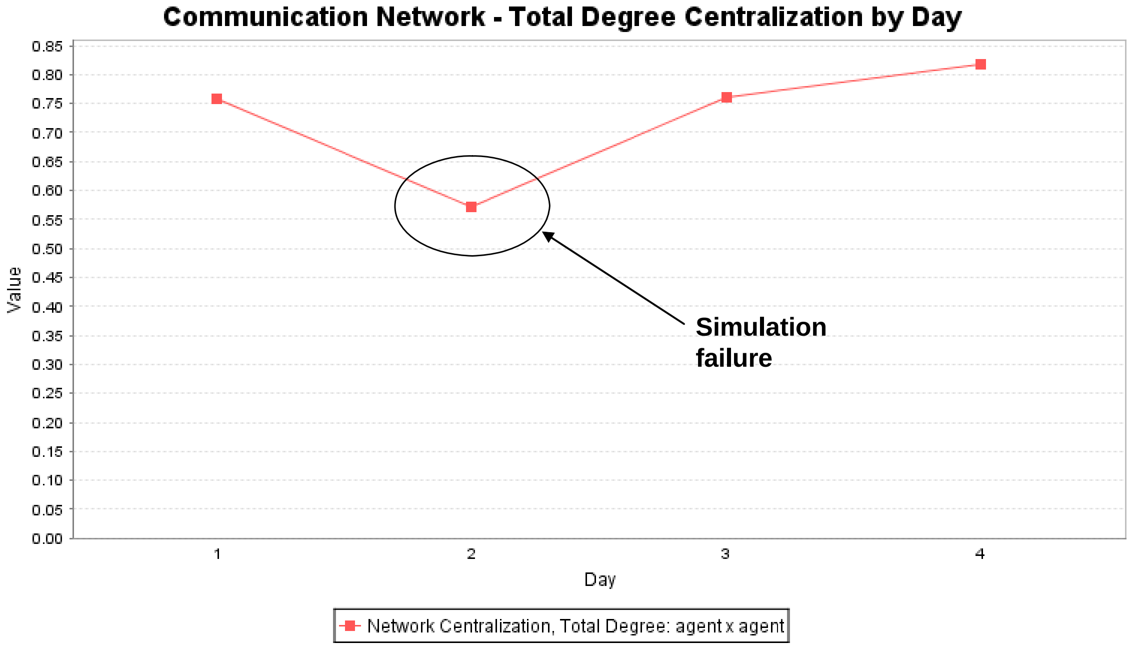

Figure 7: Communication Structure

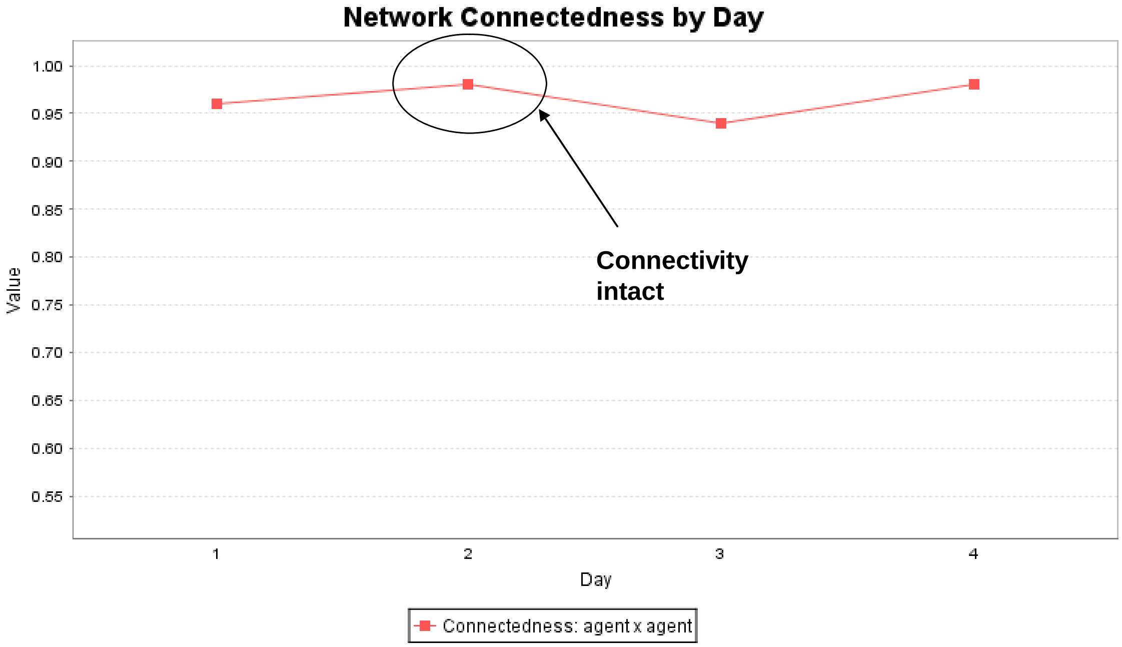

Figure 82: Network Connectedness

V. Conclusion

The OF07/DWE III simulation exercise (SIMEX) assessed the capability of a BFSB and Division staff's ability to operate in an information-rich network environment. In this experiment the True / False (T/F) probe methodology was effective at assessing how well the refined modular division was capable of conducting command and control of full spectrum operations. The methodology was also useful in measuring the BFSB's ability to answer the information requirements of the Division and conduct stability operations in their own AO.

As the results show, although limited in scope given the low sample size, the T/F Probe Methodology and S\DNA provide a unique approach to examining and understanding the effects of networking on human performance. The general declining trend in the sensitivity data may be explained by the simulation failure, but the overall similarities in the average sensitivities between the Division and BFSB can be due to their adjustment in communication and network structure.

In such a cognitively complex battlefield environment as simulated in OF07/DWE III, there are no shortages for opportunities where information can be classified as false. False information is often the result of information that is inaccurate, untimely, or incomplete. Good SA is having the ability to distinguish between true and false information and the T/F probe methodology provides a rapid and feasible measure for assessing SA in complex simulations. Likewise, an organizational network that is adaptive and resilient as observed in the S\DNA, can be beneficial at overcoming technological and network failures and the sheer volume of information in a dynamic complex environment. Together, these two methods provide analysts an approach to understanding how the complex interaction between individual SA and the organizational network affect mission effectiveness in command and control.

References

Alberts, David S., John J. Garstka, & Frederick P. Stein. *Implications for MCPs. Network Centric Warfare: Developing and Leveraging Information Superiority*, 2nd Edition (Revised). Washington, DC: DoD CCRP Publication Series, 1999.

Committee on Network Science for Future Army Applications, National Research Council. Network Science. The National Academies Press. 2005.

Edgar, G. K., Edgar, H.E., & Curry, M.B. (2003). Using signal detection theory to measure situation awareness in command and control. *Proceedings of the Human Factors and Ergonomics Society 47th Annual Meeting*.

Edgar, G.K., Smith, A.J., Stone, H.E., Beetham, D.L., & Pritchard, C., (2000). QUASA: QUantifying and Analyzing Situational Awareness. Paper presented at the IMCD People in Digitized Command and Control Symposium, RMCS Shrivenham, UK (CD-ROM).

Fredericks, B. (1997). Information Warfare: The Organizational Dimension Sun Tzu Art of War in Information Warfare Compendium, essay submitted to National Defense University's Suz Tzu Art of War in Information Warfare competition, 1997. Available via http://www.ndu.edu/ndu/inss/siws/ch4.html.

Garstka, J. and Alberts, D. (2004). Network Centric Operations Conceptual Framework Version 2.0. Washington, D.C., DoD CCRP Publication Series.

Leggatt, A. (2004). Objectively measuring the promulgation of commander's intent in a coalition effects based planning experiment (MNE3). *Proceedings of the 9th International Command and Control Research and Technology Symposium*, Copenhagen.

Luck, Gary (Gen-R). November 2006. Insights on Joint Operations: The art and science. *A Common Perspective.14 (2).*

McGuinness, B. (2004). Quantitative analysis of situational awareness (QUASA): Applying signal detection theory to true/false probes and self-ratings. *Proceedings of the 9th International Command and Control Research and Technology Symposium*, Copenhagen.

Thomas J.A. Pierce, L.G., Dixon, M.W., Fong, G. (2007). Interpreting Commander's Intent: Do we really *know* what we know and what we don't know? *Proceedings of the 12th International Command and Control Research and Technology Symposium*, Rhode Island.